



Achieving HIPAA Compliance

Presentation Objective

*To strengthen your awareness of
HIPAA's Administrative Simplification
Requirements...*

Who Can We Thank?

The 104th Congress

Sought to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.





HIPAA Requirement Review

The Health Insurance Portability and Accountability Act of 1996, Administrative Simplification, requires payers, providers, and claims clearinghouses to establish protections, adopt standards, and meet requirements for the transmission, storage, and handling of certain health care information.

CAUTION

- It's easy to get carried away with implementing
- Medical offices will implement differently
- With HIPAA, one shoe size does not fit all...

HIPAA Exemptions Exist But May Have Long-Term Implications

- A provider of services with fewer than 25 full-time equivalent employees
- A physician, practitioner (pharmacy), facility, or supplier with fewer than 10 full-time equivalent employees
- No EDI

Overall Compliance... Aim For The “Bull’s Eye” Ongoing Efforts Likely To Continue

Transactions, Code Sets, Identifiers – October 16, 2003

Privacy – April 14, 2003

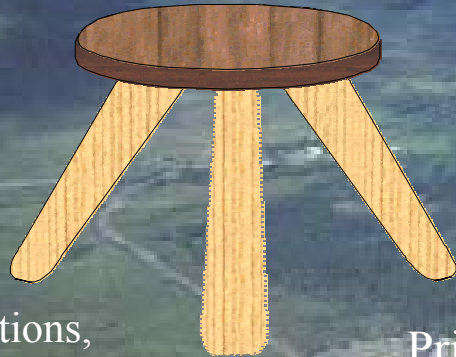
Security – April 21, 2005



Our Discussion

Administrative Simplification

Future Regulations Pending



Transactions,
Code Sets,
Identifiers

Security

Privacy

HIPAA Requires Providers To Change The Way...

- Patient information is stored
- Patient information that is sent electronically to others
- Patient information is handled

A photograph of a stone archway in a grassy field. A path leads through the archway. The text "A 'Quick' Gap Assessment – Are You Ready For Privacy?" is overlaid in the center of the image.

A “Quick” Gap
Assessment – Are You
Ready For Privacy?

Are You Ready For Privacy?

- Have you developed your notice of privacy practices?
Yes ☐ Not Yet ☐
- Does your authorization document contain the required detail for PHI disclosure?
Yes ☐ Not Yet ☐
- Are you aware of the minimum necessary requirements for disclosure of PHI?
Yes ☐ Not Yet ☐
- Can you identify when to use a business associate contract?
Yes ☐ Not Yet ☐

Are You Ready For Privacy?

(Continued)

- Are you aware of special circumstances allowing for disclosure of PHI without an authorization?

Yes ☐ Not Yet ☐

- Are you aware of the 19 elements included in PHI?

Yes ☐ Not Yet ☐

- Are you aware of products and services that represent marketing?

Yes ☐ Not Yet ☐

- Do you understand patients right to request restrictions on the use and disclosure of PHI ?

Yes ☐ Not Yet ☐

Are You Ready For Privacy?

(Continued)

- Can you accommodate individuals requesting to receive PHI communications by an alternative means?
Yes ☐ Not Yet ☐
- Are your medical files managed in a way that allows for patient inspection/release of PHI?
Yes ☐ Not Yet ☐
- Are you aware of your obligations should a patient request to amend their medical record?
Yes ☐ Not Yet ☐
- Do you document non-routine disclosure of PHI ?
Yes ☐ Not Yet ☐

Are You Ready For Privacy?

(Continued)

- Have you designated a privacy official?

Yes ☐ Not Yet ☐

- Have you trained your staff on handling PHI?

Yes ☐ Not Yet ☐

- Does your office have a way to address patient complaints?

Yes ☐ Not Yet ☐

- Do you have a policy to handle a breach in patient confidentiality?

Yes ☐ Not Yet ☐

Are You Ready For Privacy?

(Continued)

- Have you trained your staff to work with individuals that exercise their rights under the privacy regulations?
Yes ☐ Not Yet ☐
- Is your office aware that patients cannot be asked to waive their privacy rights?
Yes ☐ Not Yet ☐
- Have you developed privacy policies and procedures?
Yes ☐ Not Yet ☐
- Have you made changes in policies to maintain PHI for 6 years?
Yes ☐ Not Yet ☐

Are You Ready For Privacy?

(Continued)

- Are you familiar with the differences between consents and authorizations?

Yes ☐ Not Yet ☐

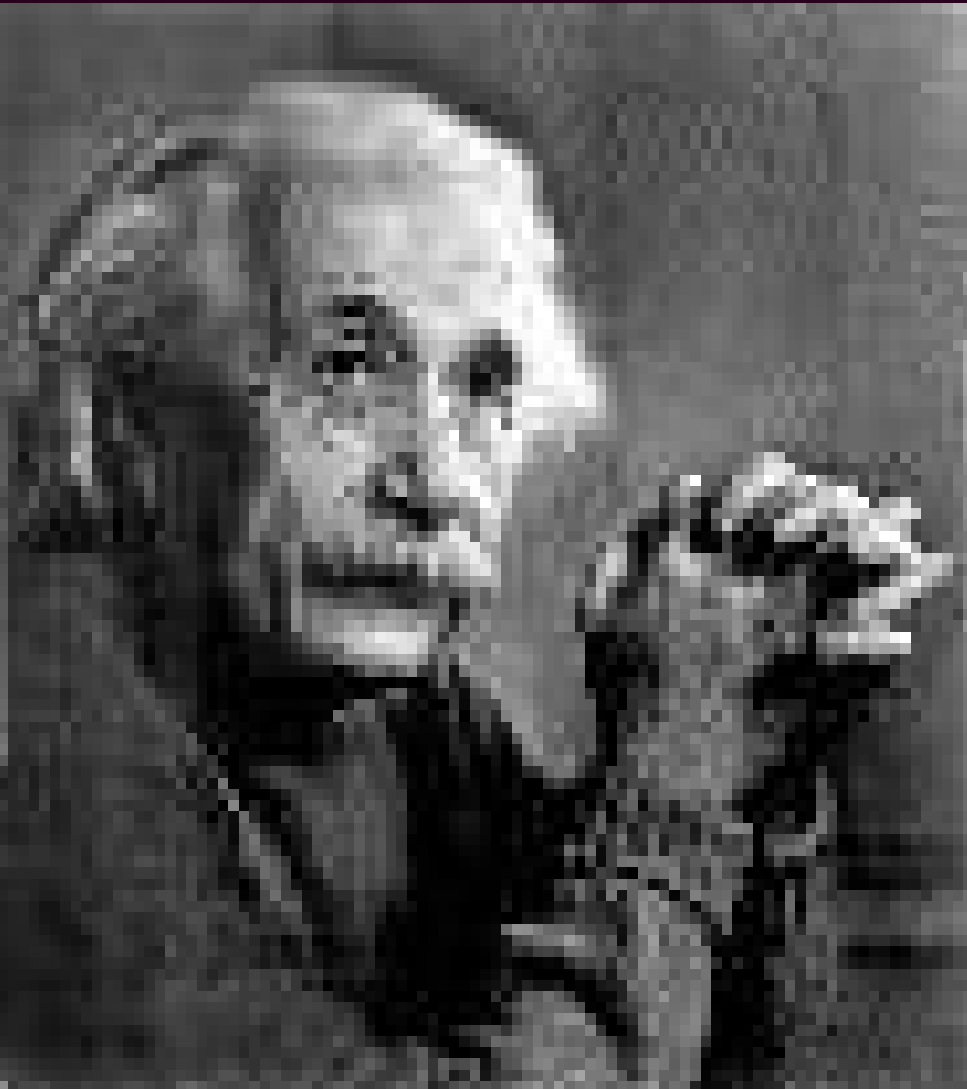
- Does your notice of privacy practices include DHHS contact information & time line for filing a complaint?

Yes ☐ Not Yet ☐

- Is your office able to respond to an unannounced audit?

Yes ☐ Not Yet ☐

How Compliant Are You With Privacy?



- Mostly compliant
 - » 20-23
- Somewhat compliant
 - » 16-19
- Not at all compliant
 - » <15

Is Full Compliance An Issue?

- CMS audits transaction standards and code sets
- Office for Civil Rights monitors privacy and security
- CNN News releases a 30 minute segment on new patient rights
- Think of your patients as your first step toward an audit

A pixelated, low-resolution image of a blue bear swimming in water. The bear is facing left, with its head and front paws visible above the water surface. The water is a dark blue-green color, and the background is a lighter green. The bear's fur is a mottled blue and white. The text is overlaid on the image in a yellow, cursive font with a white outline.

Did You Know...

Maryland Has A Privacy Law...

*An Overview & Some Leading
Examples*



Maryland Confidentiality of Medical Records Act - *Background...*

- 1978 Maryland Medical Records Act
- 1990 Confidentiality of Medical Records Act
 - » *1984 - 22 page report identified discrepancies in medical records confidentiality*
 - » *1987 - Attorney General redrafts confidentiality law for mental health records*
 - » *1989 - Health Subcommittee, of the Senate Economic and Environmental Affairs Committee drafts a detailed statutory coverage of confidentiality of medical records*
 - » *Senate Bill Number 584 signed into law on May 29,*

Federal Versus State Comparison



True or False: HIPAA is a national effort to standardize the storage, transmission, and handling of certain patient information

Category	Comparison (H) HIPAA (S) State √ More Stringent
<i>Business Associate Agreements</i>	(H) √ contracts are required when sharing patient information with a non-covered entity. (S) does not require written agreements, however, certain redisclosure provisions apply.
<i>Covered Entities</i>	(H) limited to EDI activity of payers, providers, and claims clearinghouses. (S) √ covers all health care providers – not limited to just EDI.

Federal Versus State Comparison

True or False: HIPAA is scalable to all covered entities

Category	Comparison (H) HIPAA (S) State √ More Stringent
Covered Information	(H) √ medical record, financial record and 19 individual identifiers. (S) limited to information contained in the medical record.
Disclosures - Abuse & Neglect	(H) allows for providers to report instances of suspected abuse. (S) √ compels providers to disclosure information of suspected abuse.

Federal Versus State Comparison



True or False: HIPAA enforcement should be viewed more as "a carrot and not a stick"

Category	Comparison (H) HIPAA (S) State √ More Stringent
<i>Disclosures – Family, Friend, Etc.</i>	(H) practitioner discretion unless advised otherwise by patient. (S) similar to federal requirements.
<i>Disclosures - Legally Compelled</i>	(H) allows when required by regulation (law). (S) √ defines specific types of compelled disclosures, i.e., subpoena, summons, warrant, or court order.

Federal Versus State Comparison

True or False: CMS monitors the privacy regulations and OCR monitors the transaction & code set standards

Category	Comparison (H) HIPAA (S) State √ More Stringent
Disclosure - Mandatory v. Permissive	(H) no direct provision, rather it's implied. (S) √ outlines elements for mandatory disclosure. Protections exist against litigation based on a technical violation.
Disclosure - Minimum Necessary	(H) √ only allowed to disclose minimum amount of information to accomplish task. (S) strong protections apply to mental health record disclosures.

Some Leading Reminders About Privacy

Notice Of Privacy Practices

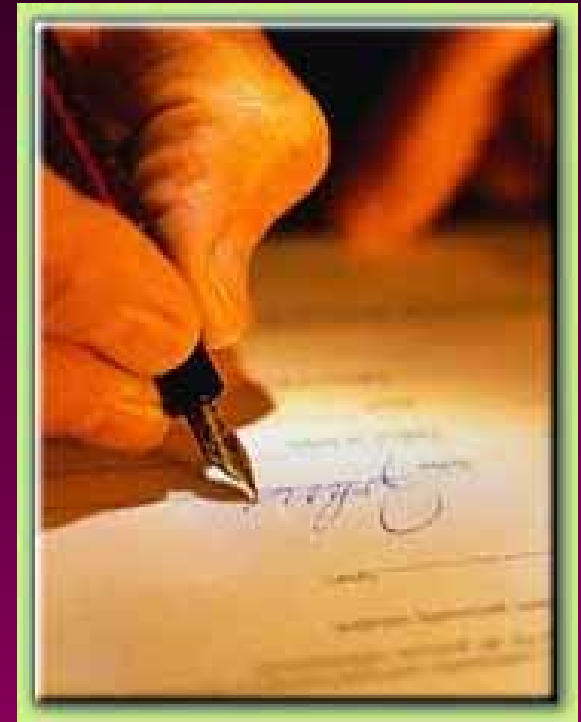
A Pivotal Point In Compliance

- An individual has the right to adequate notice of the uses and disclosures of protected health care information
- The covered entity must provide a notice that is written in plain language
- Direct treatment providers to make a good faith effort to obtain a patient's written acknowledgement of the notice
- In emergency situations, the notice must be provided as soon as is reasonably practical
- Notice can be mailed

Business Associate Contract

An Agreement Between Parties

- Acts on behalf of a covered entity in conducting activities involving use of PHI
- Covered entities are not responsible for actions of business associates
- Monitoring is not required
- An organization can be both a covered entity and a business associate
- Due April 04 (renewing contracts)



Protected Health Information

Medical Record, Financial Record & 19 Identifiers

- Name
- Address
- E-mail
- Dates
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate Number
- License Number
- Vehicle Identifiers
- Facial Photographs
- Telephone Numbers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Geographic Units
- Any Other Unique Identifier Or Codes

Consent - Optional

- A consent allows a provider to use or disclose protected health care information to carry out treatment, payment, & health care operations
- One time only:
 - Inform that protected health information may be used or disclosed for treatment, payment, or health care operations
 - Refer to notice of privacy practices
 - State the right to request restrictions
- May condition treatment based on consent
- May be revoked
- Provider must document & retain consent forms
- Attempts to obtain a consent must be documented

Authorization

Think About Your Needs

- Authorization is more detailed and specific than consent
 - Limited to only information to be disclosed
 - Recipient of information
 - Includes an expiration date
- Core elements of a valid authorization:
 - A description of the information to be used or disclosed
 - The name or other specific identification of the person authorized to make the requested uses and disclosures
 - An expiration date or expiration event
 - A statement of the individuals right to revoke the authorization in writing
 - A statement that information used or disclosed may be subject to re-disclosure by the recipient
 - Signature of the individual and date

Marketing

Some Clarification

- A covered entity may not disclose or use PHI for marketing without an authorization
- Exception to the marketing rule applies to:
 - » Face to face encounters
 - » Products of services of nominal value
 - » Health-related products and services
- PHI can be disclosed to a business associate that assists in communications

Marketing As Fund Raising

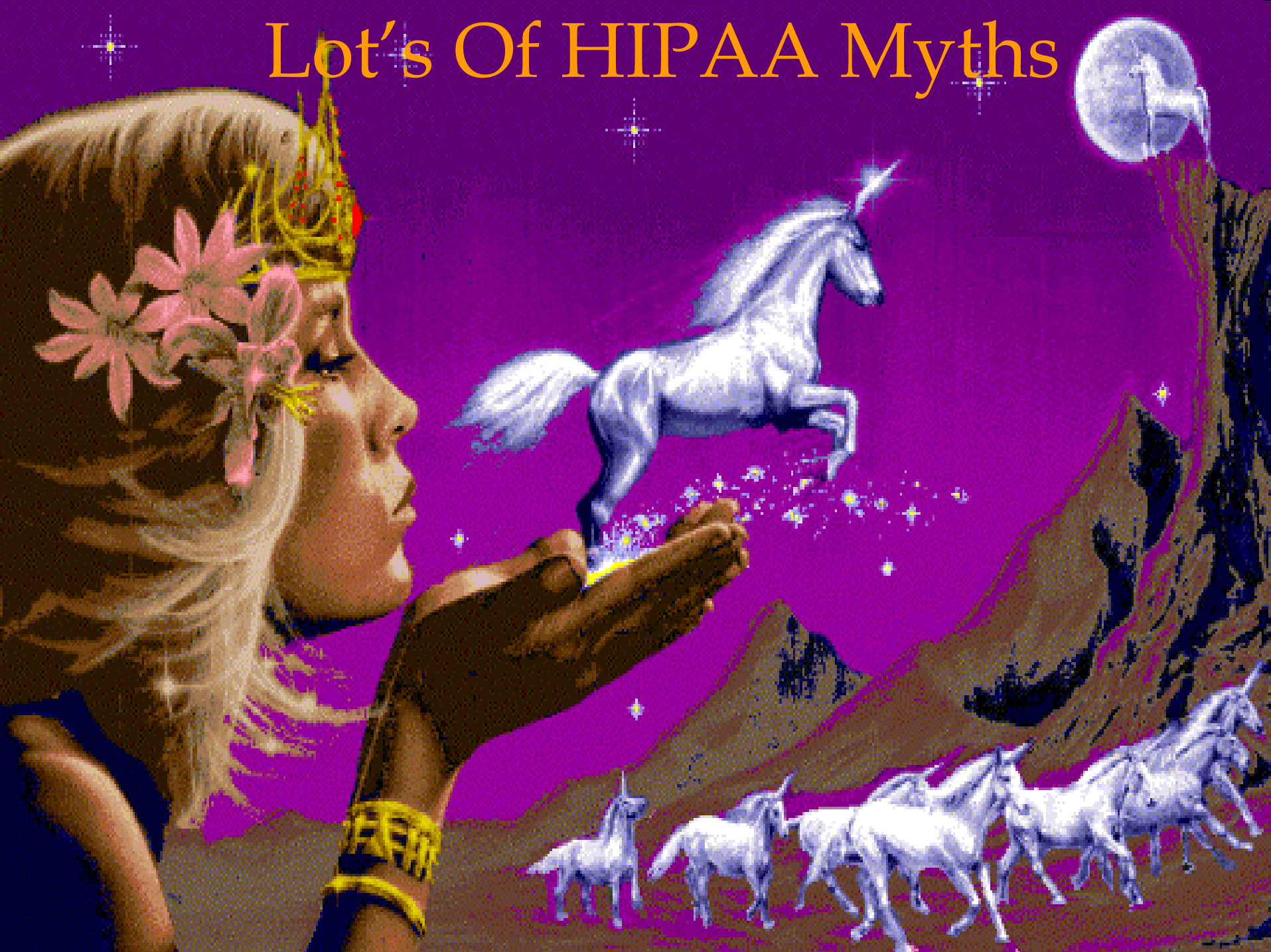
An Area Often Overlooked

- The covered entity may use or disclose PHI to a business associate or to an institutionally-related foundation for the purposes of raising funds for its own benefit without an authorization
- PHI used for fundraising must be limited to demographic information and dates of health care provided to an individual
- All fundraising activities must be included in the notice of privacy practices
- All fundraising material must include information on how an individual may opt out of receiving future notification
- The covered entity must take steps to ensure that individuals that opt out are not sent future information

Providers Worry...

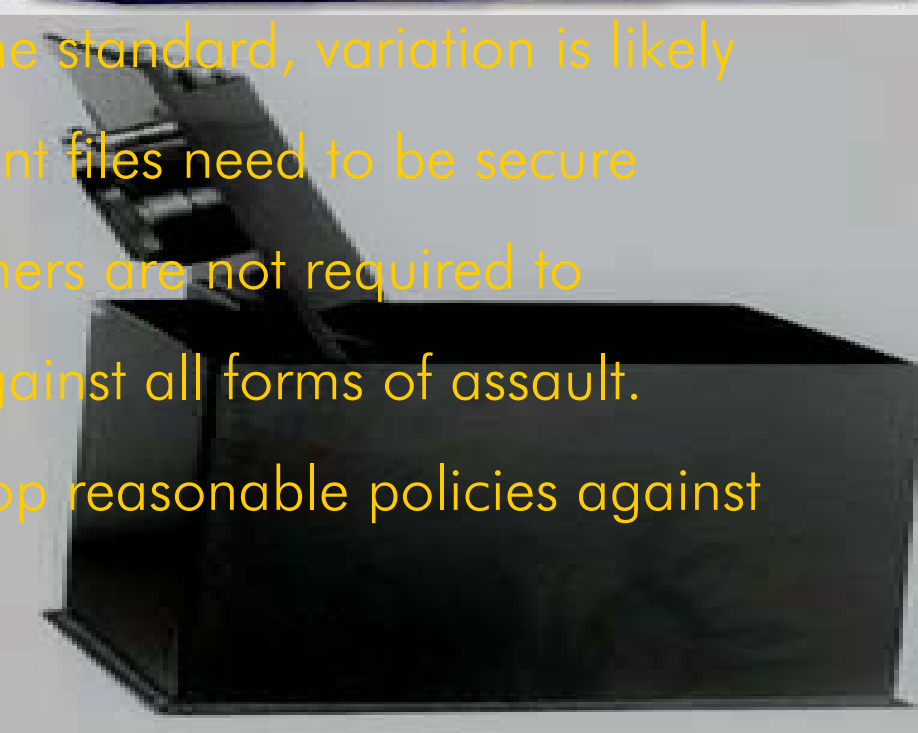
- Charts on exam room doors
- Charging patients for a copy of their medical record
- Leaving appointment reminders on answering machines
- Managing the use of temporary office staff
- Leaving medical charts in physicians offices
- Work that's defined as "in progress"

Lot's Of HIPAA Myths



Protecting Patient Information What's Really Required?

The regulations do not describe the particular measures a covered entity must take to meet the standard, variation is likely to exist among practitioners. Patient files need to be secure within a secure location. Practitioners are not required to guarantee the protection of PHI against all forms of assault. Practitioners are required to develop reasonable policies against theft of PHI.



Sign In Sheets – Okay To Use



- HIPAA does not require providers to use patient tacking sheets
- Consider its purpose and value
- Look for opportunities to limit potential disclosure of PHI
- Evaluate low cost alternatives



Shredders – Their Value To Providers



Protecting Anonymity In Waiting Rooms--- Is This Possible?



Confidential Communications – *Discretion Is Important*

- Manage to your patients expectations
- Use discretion when communicating over the telephone or counter
- Respect privacy rights of your patients even when they forget too

Administrative Tasks

A Reminder...

- Designate a privacy official
- Develop policies and procedures
- Create the notice of privacy practices
- Train employees

Patient Awareness - Not Too Far Off...

- Right to inspect and copy protected health information
- Right to amend
- All approve uses and disclosures
- Right to an accounting of disclosures
- Right to have reasonable requests for confidential communication accommodated
- Right to file a written complaint
- Right to receive written notice of information practices



A Word About The Transaction Standards

Plan Wisely For October...

Transactions Can Generate A Cost-Savings

- Average saving per transaction
 - » Practitioners – 35 percent
 - » Hospitals – 15 percent
- Acceleration of payment on claims (approximately 28 days on average)
 - » Hospitals – 44 percent improvement of the cash flow
 - » Practitioners – 52 percent improvement of the cash flow

Source: Hansen, Healthcare Financial Management, Nr. 1 (1999), 64-66

Look At How Well Private Payers Are Doing...

Percent Processed Without Manual Intervention

<u>Provider</u>	<u>HMO</u>	<u>Non-HMOs</u>	<u>Total</u>
● Hospitals	9.0	26.7	19.9
● Practitioners	18.4	28.2	25.4
● Total	17.1	28.0	24.8

HIPAA Transactions

Identify Those You Plan To Use

- Using the transactions produces administrative savings:
 - Enrollment in a health plan,
 - Eligibility for a health plan,
 - Health claims (retail drug, dental, professional, and institutional)
 - Health care payment & remittance advise
 - Health plan premium payments,
 - Health claim status,
 - Referral certification, authorization, coordination of benefits (Rx: NCPDP Telecommunication Guide)

Complying With The Transactions...

- Use caution in relying on your software vendor's word regarding system compliance
- Using a testing certification vendor is highly recommended
 - » Claredi, EDICECS, Foresight Corporation, Applabs
- Follow up with your software vendor periodically for new releases

HIPAA Security

A New Concept On
The Horizon...

HIPAA Security Standards

Final Rule Different Than Proposed Rule

Three Broad Security Categories

- Administrative Safeguards

Development and implementation of security measures to protect data, and the conduct of personnel in relations to the protection of data

- Physical Safeguards

The protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as intrusion

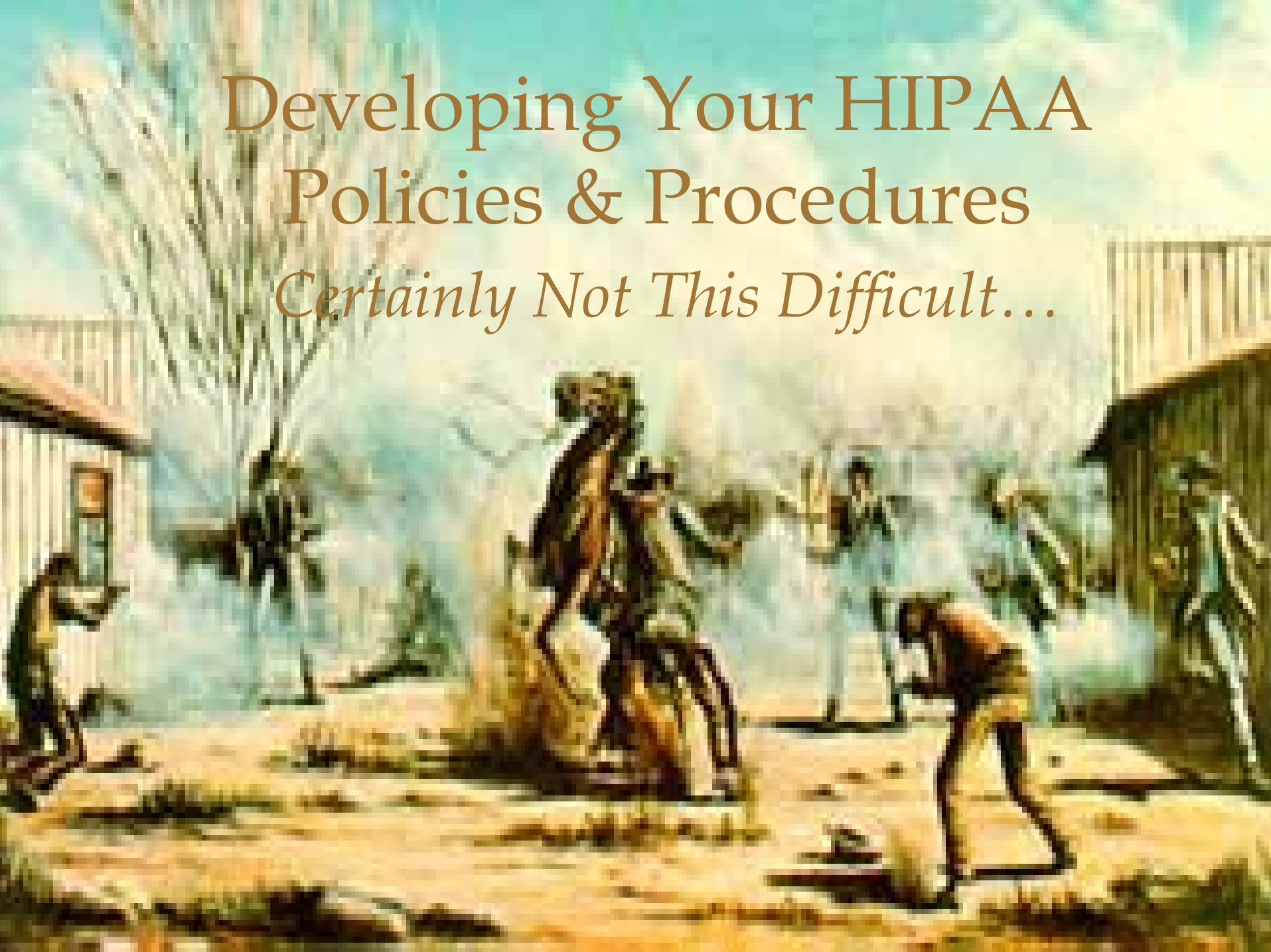
HIPAA Security Standards

(Continued)

- Technical Safeguards

The process that's put into place to protect information and to control and monitor individual access to information

Developing Your HIPAA Policies & Procedures *Certainly Not This Difficult...*



Sound Documentation Is Essential

- Transaction Standards & Code Sets
- Privacy
- Security



Policies and Procedures

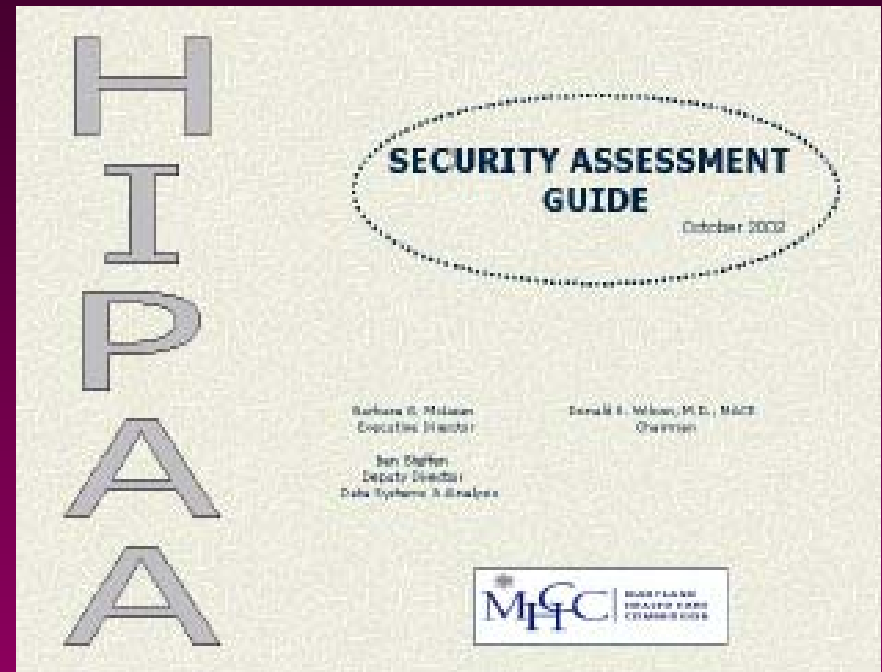
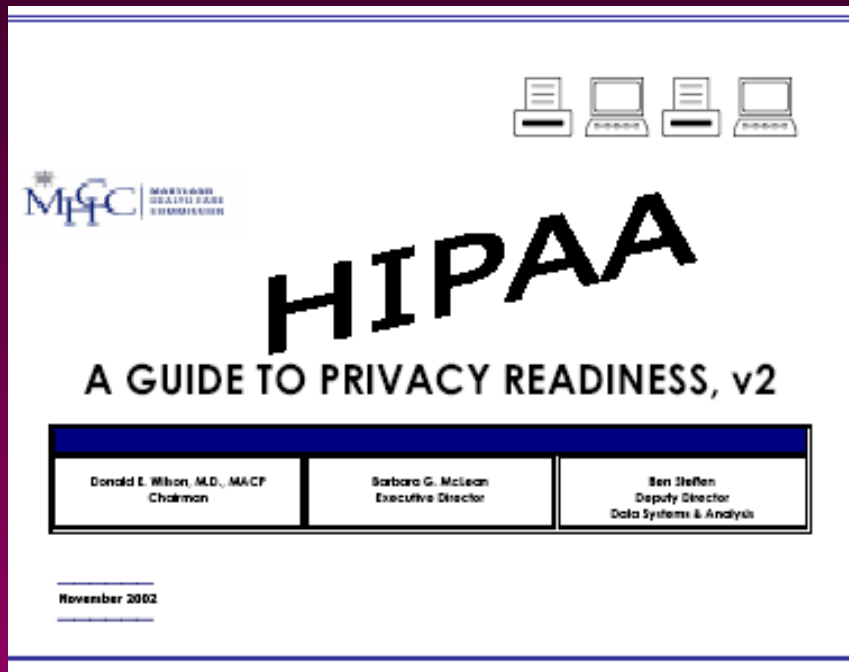
Preparing Your Documentation

- Transaction Standards
 - Vendor self-certification letter or third party certification (include specific transactions)
- Privacy
 - Gap assessment: Q&A
 - Policies and procedures
 - Sample forms
 - Training log
- Security
 - Gap assessment: Q&A
 - Policies and procedures
 - Sample forms
 - Training log
- Ongoing review of your compliance manual is required

HIPAA Compliance Tools

Both are available at the MHCC Web-site:

WWW.MHCC.State.MD.US





MHCC HIPAA Tools: What You Can Expect To Find

Privacy tool contents:

- *Introduction*
- *Maryland Law on the Confidentiality of Medical Records*
- *HIPAA Definitions*
- *Assessment Guide and Work Plan*
- *Business Associate Contract (illustrative document)*
- *Chain of Trust Partner Agreement (illustrative document)*
- *Notice of Privacy Practices (illustrative document)*
- *Computer and Information Usage Agreement (illustrative document)*


Security tool contents:

- *Introduction*
- *Definitions*
- *Small Provider Implementation Example*
- *Assessment Guide and Work Plan*
- *Administrative Procedure Checklist*
- *Physical Safeguards Procedures Checklist*
- *Technical Security Services Procedures Checklist*
- *Technical Security Mechanisms Procedures Checklist*

Imagine A Time Period When...

- Patients only seek care from providers that are HIPAA compliant
- Liability carriers insure based upon HIPAA compliance
- Financial institutions underwrite loans/lines of credit based upon HIPAA compliance

Lasting Thoughts...

- 
- Other final rules expected to be released
 - Ongoing modifications of existing rules likely to occur
 - Continue to become “HIPAA Wise”
 - Implementation dates are “start dates” not “end dates”

For More Information on HIPAA

Official Sites

Government sites:

<http://aspe.hhs.gov/admnsimp> - Department of Health and Human Services

<http://www.hcfa.gov/security/iseclplcy.htm> - HCFA Internet Security Policy

<http://www.wpc-wdi.com/hipaa> -- Implementation Guides

Non-govt sites:

<http://www.wedi.org>

<http://www.nchica.org>

<http://www.hipaadvisory.com/>

MHCC site:

<http://www.mhcc.state.md.us>



